Actualiteiten België

Werkten mee aan 'Actualiteiten' voor België:

Niels Vandezande (NV) en Els Kindt (EK), beiden onderzoeker, Interdisciplinary Center for Law & ICT, K.U.Leuven, Dirk De Bot (DDB) met Bijzondere Doctoraatsbeurs FWO Vlaanderen, onderzoeker Center for Law, Science, Technology & Society Studies (LSTS), Vrije Universiteit Brussel en Bastiaan Bruyndonckx (BB), advocaat Balie Brussel

Coördinatie en editing: Els Kindt

Privacy Algemeen

234

Publieke consultatie *cybersurveillance* door werkgevers

Op 13 juli 2011 heeft de Belgische Commissie voor de bescherming van de persoonlijke levenssfeer ('CBPL') via haar website een publieke consultatie gelanceerd in verband met *cybersurveillance* of in het Nederlands: werkgeverscontrole op internet- en e-mailgebruik door werknemers.

Zoals men weet, heeft de CBPL zich in het verleden reeds meer dan eens uitgesproken in publieke adviezen omtrent de problematiek van *cybersurveillance*. Daarnaast ontvangt de CBPL zeer regelmatig vragen van verschillende partijen (werkgevers, werknemers, vakbonden, *privacy-officers*, rechtspractici e.d.) omtrent dit onderwerp, hetgeen de gevoeligheid ervan aantoont.

Daarbovenop komt dat, niettegenstaande de bestaande adviezen van de CBPL, er heel wat vragen bleven bestaan omtrent het samenspel tussen de verschillende rechtsregels van toepassing inzake *cybersurveillance*, waaronder de interactie tussen de regels inzake de bescherming van persoonsgegevens (de Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en de Collectieve arbeidsovereenkomst nr. 81 van 26 april 2002 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische onlinecommunicatiegegevens) enerzijds en de regels inzake de bescherming van het telecommunicatiegeheim (artikel 314bis van het Strafwetboek en artikel 124 e.v. van de Wet van 13 juni 2005 betreffende de elektronische communicatie) anderzijds.

In haar 'verantwoordingstekst' bij de publieke consultatie verwijst de CBPL uitdrukkelijk naar de 'vertwijfeling' waarvan sommige vragen en situaties die haar worden voorgelegd, getuigen. Ten eerste zou, volgens sommige analyses, geen onderscheid mogelijk zijn tussen *professioneel* en *privaat* gebruik van de telecommunicatiemiddelen van de werkgever, waardoor de meest absolute bescherming dus permanent gegarandeerd zou moeten worden, ongeacht de aard van het gebruik. Ten tweede zou de *individuele toestemming* (vrij, specifiek en wel geïnformeerd) van alle bij de telecommunicatie betrokken fysieke personen steeds vereist zijn om kennis te kunnen nemen van een bepaalde informatie (verkeer, inhoud …) gelieerd aan het patronale telecommunicatiemiddel. Ten slotte zou, aldus bepaalde auteurs, de CAO nr. 81 die de controle van het (privé)gebruik van de patronale telecommunicatiemiddelen omkadert, ingaan tegen de vereisten van hogere rechtsnormen en derhalve als nietig moeten worden beschouwd.

Om voormelde redenen heeft de CBPL het initiatief genomen de *cybersurveillance*-problematiek opnieuw grondig onder de loep te nemen, hetgeen is uitgemond in een omvangrijk dossier dat wordt onderworpen aan een publieke consultatie die loopt tot 30 november 2011. Het dossier van de CBPL bestaat, naast een publieksnota of verkennende stellingname, uit (1) een voorwoord, (2) een introductietekst, (3) een verantwoordingstekst, (4) een uitgebreid juridisch rapport en, tenslotte, (5) een aantal aanbevelingen.

De teksten die de CBPL in het kader van de publieke consultatie *cybersurveillance* publiceerde, hebben zeker een aantal verdiensten.

Voor de eerste maal onderzoekt de CBPL in een omvattend rapport de *cybersurveillance*-problematiek vanuit alle verschillende juridische invalshoeken en poogt zij de vaak conflicterende rechtsregels inzake de bescherming van persoonsgegevens, de bescherming van het telecommunicatiegeheim, de controle op onlinecommunicatiegegevens van werknemers zoals vastgelegd in CAO nr. 81, het patronale gezag zoals vastgelegd in de Wet van 3 juli 1978 betreffende de arbeidsovereenkomsten en inzake externe en interne hacking (artikel 550bis Strafwetboek) met elkaar te verzoenen. Daarbij erkent de CBPL dat de huidige problematiek c.q. impasse deels het gevolg is van het 'onbuigzame' advies nr. 10/2000 van 3 april 2000 uit eigen beweging betreffende het toezicht door de werkgever op het gebruik van het informaticasysteem op de werkplaats. Volgens de CBPL is het achterliggende juridische kader inmiddels grondig van gedaante veranderd, waardoor een herziening van haar advies nr. 10/2000 van 3 april 2000 zich opdringt.

Eén van de grote verdiensten van de gepubliceerde teksten is dat de CBPL uitdrukkelijk erkent dat de toegang door de werkgever tot elektronische communicatiegegevens van werknemers verschillende doeleinden kan beogen. Tot nog toe is de meeste inkt gevloeid over het gebruik van systemen die uitdrukkelijk tot doel hebben de werknemer te controleren op *abusief privatief gebruik* van de door de werkgever ter beschikking gestelde informaticasystemen. Daarnaast bestaan er echter tal van situaties waarin de werkgever een legitiem belang heeft toegang te krijgen tot bepaalde elektronische communicatiegegevens van *professionele aard* van werknemers teneinde de continuïteit van de dienstverlening en de goede werking van de onderneming te verzekeren, inzonderheid in geval van afwezigheid, overlijden of het vertrek van een werknemer. Aldus introduceert de CBPL een dubbel onderscheid, naargelang de *aard* van de informatie (*privé* informatie versus *professionele* informatie) en naargelang de *finaliteit* van de werkgeverstoegang (*controle* van de werknemers versus

continuïteit van de dienstverlening en goede werking van de onderneming).

Wat het conflict tussen de regels tot bescherming van het telecommunicatiegeheim en de regels inzake de bescherming van persoonsgegevens betreft, zullen vele rechtspractici met plezier lezen dat, althans volgens de CBPL, het gezagsrecht van de werkgever zoals neergelegd in de Wet van 3 juli 1978 betreffende de arbeidsovereenkomsten voor de private sector of in de rechtspositie van ambtenaren voor de publieke sector, een voldoende wettelijke grondslag vormt om bepaalde controlehandelingen te stellen, voor zover die dan gebeuren conform de normaal gangbare bedrijfsvoering en conform andere toepasselijke wettelijke en reglementaire bepalingen. Aldus zou de werkgever zich kunnen beroepen op de uitzonderingsbepaling van artikel 125, 1° van de Wet betreffende de elektronische communicatie om te ontkomen aan de strafbaarstellingen van artikel 124 van de Wet betreffende de elektronische communicatie en artikel 314bis van het Strafwetboek.

Anderzijds spreekt de CBPL zich op verscheidene plaatsen in de gepubliceerde teksten uit *tegen* het beroep door de werkgever op een van de werknemer verkregen *toestemming*. De CBPL stelt uitdrukkelijk dat, hoewel sommige rechtspraak toch belang schijnt te hechten aan dergelijke toestemming, deze toestemming moeilijk kan worden beschouwd als 'vrij' in de zin zoals vereist door de wet. Volgens de CBPL genieten andere rechtsgronden bijgevolg de voorkeur, boven de individuele toestemming van de werknemer.

De CBPL hecht tevens veel belang aan de naleving van CAO nr. 81 van 26 april 2002 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische onlinecommunicatiegegevens. Opvallend is de stelling van de CBPL dat ook werkgevers uit de openbare sector *de facto* onderworpen zijn aan de CAO nr. 81 nu het hier immers vooral gaat om een concretisering van de na te leven principes van de Wet verwerking persoonsgegevens voor toezicht op *persoonlijke* elektronische communicatiegegevens. Uit de teksten van de CBPL valt anderzijds echter af te leiden dat de CAO nr. 81 voornamelijk – indien niet uitsluitend – een rol moet spelen wanneer de werkgever zich toegang wenst te verschaffen tot elektronische communicatiegegevens van de werknemer met het doel de werknemer te *controleren* op *abusief privatief gebruik* van de door de werkgever ter beschikking gestelde informaticasystemen. De bekommernis van CAO nr. 81 'betreft in hoofdzaak het surfen en mailen door werknemers voor persoonlijke doeleinden', aldus de CBPL.

De belangrijkste aanbeveling van de CBPL is dan ook het *dubbel gebruik* (zowel privé als professioneel) van het door de werkgever ter beschikking gestelde e-mailsysteem te vermijden, zodanig dat het probleem van de directe toegang tot privé-e-mail van werknemers zich niet meer zou stellen. Indien de werkgever in de*ICT-policy* heeft opgelegd dat het dubbel gebruik van zijn e-mailsysteem is verboden, dan mag de werkgever er in principe van uitgaan dat e-mails een beroepskarakter hebben, zeker ten aanzien van verzonden berichten. Wanneer werkgevers niet kunnen of willen afstappen van het dubbel gebruik van hun e-mailsysteem, zullen zij – aldus de CBPL – onvermijdelijk moeten aanvaarden dat een personeelslid een hogere privacyverwachting kan laten gelden over zijn elektronische postbus. In dat geval zal toepassing moeten worden gemaakt van CAO nr. 81. De overige aanbevelingen van de CBPL zijn vooral doch niet uitsluitend van toepassing op werkgevers die het dubbel gebruik van hun e-mailsystemen toelaten of gedogen.

Zoals vermeld, loopt de publieke consultatie tot 30 november 2011. Alle vragen, opmerkingen en reacties kunnen schriftelijk aan de CBPL worden bezorgd, hetzij per e-mail (<commission@privacy commission.be>), hetzij per gewone post (CBPL, Hoogstraat 139, 1000 Brussel). Op 16 december 2011 is er een studienamiddag gepland tijdens dewelke de CBPL een eerste overzicht en een sneuveltekst zal voorstellen. (BB)

Bron: Commissie voor de Bescherming van de Persoonlijke Levenssfeer, Publieke consultatie cybersurveillance, <www.privacycommission.be/nl/new/topic/publieke-consultatieronde-cybersurveillance.html en aldaar aangehaalde documenten>

235

Privacycommissie doet aanbevelingen inzake het gebruik van de identiteitskaart

De Commissie voor de bescherming van de persoonlijke levenssfeer ('CBPL') publiceerde in mei 2011 uit eigen beweging aanbevelingen inzake het gebruik van de elektronische identiteitskaart ('eID'). In het negen pagina's tellende document legt de CBPL uit wat wel en niet kan. De Commissie maakte hierbij een onderscheid tussen de voorlegging van de eID, het verstrekken van een kopie daarvan en het (uit)lezen van de kaart.

De CBPL stelt vooreerst duidelijk dat in de openbare sector, een persoon enkel kan verplicht worden om zijn identiteitskaart voor te leggen in de gevallen bepaald in het Koninklijk Besluit van 25 maart 2003. Het gaat dan meer bepaald wanneer de politie erom verzoekt, bij aangifte of verzoek om een attest, bij een tussenkomst van een gerechtsdeurwaarden of in het algemeen wanneer dat noodzakelijk is om de identiteit van een persoon vast te stellen.

In de private sector kan voorlegging slechts gevraagd worden indien een wettelijke bepaling daarin voorziet (bijvoorbeeld, de wettelijke bepalingen inzake de registratie van reizigers in een toeristisch verblijf) of indien dit noodzakelijk is. De CBPL benadrukt hierbij dat in talrijke gevallen, de voorafgaandelijke identificatie van een klant in de privésector niet noodzakelijk is om het contract te kunnen uitvoeren. De CBPL maakt hierbij – om voor ons onduidelijke en onnodige redenen – een onderscheid tussen contracten waarbij de uitvoering onmid-

dellijk gebeurt en contracten waarvan de uitvoering opeenvolgende prestaties vereist, waarbij in het laatste geval wel identificatie nodig zou zijn. De CBPL laat verder toe dat in het kader van een getrouwheidssysteem, bijvoorbeeld voor het verkrijgen van kortingen van winkels, de eID wordt uitgelezen voorzover de voorafgaande, geïnformeerde, vrije en specifieke toestemming werd verkregen van de klant. Tegelijkertijd moet aan de klant wel een alternatief worden geboden voor het gebruik van zijn identiteitskaart.

De CBPL stelt verder dat indien de eID wordt gelezen, die gegevens uitsluitend mogen worden verwerkt en bewaard die strikt noodzakelijk zijn voor de nagestreefde doeleinden. Bovendien is steeds de machtiging vereist van het Sectoriaal comité van het Rijksregister om het Rijksregisternummer te gebruiken, zelfs in gecodeerde vorm.

De voorlegging en het uitlezen van de eID wordt verder onderscheiden van het toestaan van het nemen van een kopie van de eID. De CBPL bepaalt dat het nemen van een kopie enkel kan in de door de wet voorgeschreven gevallen. De CBPL raadt aan om indien een kopie wordt overhandigd, men een doorstreepte kopie afgeeft, met vermelding van de bestemmeling en het toegestane gebruik. Deze gevallen waarbij het nemen van een kopie zou toegestaan worden, zijn te bepalen door de wetgever en zouden door de wetgever moeten beperkt worden waar noodzakelijk voor redenen van openbaar belang.

De CBPL raadt ook sterk af om identiteitskaarten in bewaring te geven of te nemen, een meer en meer voorkomende praktijk.

De aanbevelingen worden afgesloten met de aanmoediging van anonieme gegevensverwerkingen aan de hand van de eID, zoals het nagaan van de woonplaats zonder betrokkene evenwel te identificeren.

De CBPL benadrukt dat naast deze bijzondere aanbevelingen, ook alle andere bepalingen van de Wet verwerking persoonsgegevens van toepassing blijven, waaronder de informatieplicht en de verplichting om passende organisatorische en technische maatregelen te nemen. (EK)

Bron: CBPL, Aanbeveling 03/2011 van 25 mei 2011 uit eigen beweging over het nemen van een kopie van de identiteitskaart en over het gebruik en de elektronische lezing ervan, 9 p. beschikbaar op <www.privacycommission.be>

236

Geen geest, maar zand in de machine – een alarmkreet van de voorzitter van de Belgische Commissie voor de bescherming van de persoonlijke levenssfeer

Recent heeft de voorzitter van de Belgische Commissie voor de bescherming van de persoonlijke levenssfeer (verder de Privacycommissie) in een interview de alarmklok geluid over de werking van de toezichthoudende autoriteit inzake gegevensbescherming in België. Die kreet houdt in belangrijke mate verband met de aanslepende politieke situatie in België. Ook al is de politieke situatie wat minder stabiel sinds 2007, ze geeft, wat de Privacycommissie betreft, pas echt problemen sinds juni 2010. Sinds dat ogenblik is er in België geen echte regering meer, maar enkel een regering in lopende zaken, waarvan de bevoegdheden over het algemeen beperkend omschreven. Zo stelt men onder meer dat een regering in lopende zaken geen benoemingen kan doorvoeren. Eén van de gevolgen hiervan is dat de samenstelling van de Privacycommissie nog (steeds) niet kon hernieuwd worden. Het mandaat van de huidige Privacycommissie liep ten einde op 4 december 2010. Voor de hernieuwing van de samenstelling dient de wettelijk voorziene procedure te worden gevolgd. Dit houdt in dat de kandidaat-leden worden gekozen door de Kamer van volksvertegenwoordigers uit lijsten die door ministerraad worden voorgedragen en die voor elk van te bekleden mandaten twee kandidaten bevatten. Het probleem situeert zich bij de voordracht van de kandidatenlijst. Van een regering in lopende zaken wordt aangenomen dat zij geen leden kan voordragen. Gevolg hiervan is dat het mandaat van de huidige leden (willens nillens) blijft doorlopen, ook al zijn er twee leden die met pensioen willen gaan, … en dat de Privacycommissie de facto werkt met de handrem op. De voorzitter geeft immers aan dat het niet de bedoeling is of kan zijn om de nieuw samengestelde commissie te belasten met strategische beslissingen die door de vorige commissie zijn genomen. Vandaar het beeld van de handrem, die ertoe leidt dat de Privacycommissie geen nieuwe initiatieven meer neemt (kan nemen). Bij dit alles kan men overigens ook de vraag stellen of de Privacycommissie in haar huidige samenstelling nog wel op een rechtsgeldige manier kan functioneren. Het bij wet bepaalde mandaat van zes jaar is immers voorbij. Wellicht moet men hier stellen dat de uitzonderlijke omstandigheden rechtvaardigen dat ook de Privacycommissie de 'lopende zaken' behandelt.

Deze situatie heeft met name tot gevolg dat op meerdere domeinen niet de gewenste (en noodzakelijke) vooruitgang kan worden geboekt. Daarbij springen vooral de toegang tot de 'supercomputer' van de federale politie, de wetgeving rond de verwerking van persoonsgegevens in belastingszaken en de bewaring van gegevens door telecombedrijven in het oog.

Dit alles leidt ertoe dat de legitimiteit van de Privacycommissie in vraag wordt gesteld binnen Europa. De voorzitter stelt dat zijn collega's hem zien als 'de woordvoerder van een commissie waarvan het mandaat afloopt (of al afgelopen is), die spreekt voor een land in ontbinding'.

In het interview geeft de voorzitter verder ook uiting aan zijn bezorgdheid voor de toekomst. Hij verwacht de komende twee jaren 'geen cent meer te krijgen' voor nieuwe initiatieven, zoals de oprichting van een afdeling inspectie. Nochtans is deze (nieuwe) afdeling hoogst noodzakelijk. In de huidige omstandigheden zijn er immers weinig tot geen mogelijkheden om bij verantwoordelijken voor de ver-

werking enige inspectie te verrichten, waarbij de voorzitter zelf aangeeft dat de inspecties veeleer 'op een amateuristische' manier gebeuren. Zo is het vandaag blijkbaar zelfs niet mogelijk om bij de vaststelling dat een gemeenteambtenaar constant de gegevens van dezelfde persoon opzoekt in het Rijksregister, ter plekke te gaan om te zien wat het probleem is. Nochtans is zo'n onderzoek van individuele dossiers één van de taken van elke volwassen toezichthouder, wat mag blijken uit de praktijk in de buurlanden. Zo'n inspectie- en controledienst moet, volgens de voorzitter, niet meer dan een viertal medewerkers omvatten. Maar dat vereist middelen, al is het maar voor de betaling van het loon van die medewerkers. Die zijn er niet alleen niet op dit ogenblik, maar wellicht ook niet in de toekomst.

Dat alles doet de voorzitter besluiten dat de Privacycommissie, die zich sinds haar oprichting goed heeft ontwikkeld, wat aan haar lot wordt overgelaten … wat ertoe leidt dat er 'zand in de machine' komt. En iedereen weet waar dat toe leidt. (DDB)

Bron: N. Vanhecke, 'Er zit zand in de machine' – interview met de voorzitter van de Privacycommissie, Standaard Online 18 juli 2011

Bescherming persoonsgegevens

237

De Kruispuntbank van de rijbewijzen

Zoals eerder bericht in deze rubriek (zie *P&I* 2010-1), zal België ter omzetting van de Europese Richtlijn 2006/126/EG het Europese rijbewijs invoeren. Naast het harmoniseren van het rijbewijsmodel binnen de Europese Unie, heeft die richtlijn ook tot doel het invoeren van een centrale nationale databank waarin allerlei gegevens verzameld worden met betrekking tot de bestuurder, de geldigheid van diens rijbewijs en de eventuele intrekking daarvan. Dergelijke nationale databanken van de Europese lidstaten zullen vervolgens onderling verbonden worden, om grensoverschrijdende consultatie van de in deze databanken opgeslagen gegevens mogelijk te maken.

De Belgische databank van rijbewijzen werd bij Wet van 14 april 2011 ingevoerd onder de naam 'Kruispuntbank van de rijbewijzen' ('Kruispuntbank'). Naast het vaststellen van de doeleinden waarvoor de gegevens in deze Kruispuntbank gebruikt kunnen worden en het aanwijzen van de verantwoordelijke voor de verwerking van persoonsgegevens in de databank, bepaalt de wet ook de gegevens die in de Kruispuntbank verwerkt zullen worden en waarbij de Kruispuntbank als authentieke bron zal dienen. Hiermee wil de wetgever ook het principe van de unieke gegevensinzameling invoeren in deze materie. Onder de gegevens in de Kruispuntbank bevinden zich ook gegevens met betrekking tot de medische geschiktheid van de bestuurder, die nodig zijn voor de geldigheid van het rijbewijs. Hiermee kunnen ordediensten over het hele Europese grondgebied bij controle nagaan of een bestuurder medisch geschikt bevonden werd tot het besturen van zijn voertuig. Samenhangend hiermee kan – krachtens Richtlijn 2006/126/EG – de geldigheidsduur van het rijbewijs beperkt worden om vaker medische controles uit te voeren. Hoewel er een duidelijke vraag is naar meer frequente controles van de medische geschiktheid van bestuurders – onder meer door het Belgisch Instituut Voor de Verkeersveiligheid (BIVV) (zie *P&I* 2011-2) – heeft België tot op heden nog geen initiatief hiertoe genomen. Voor het gebruik van de gegevens in de Kruispuntbank zal een voorafgaande machtiging verkregen moeten worden van het Sectoraal comité voor de federale overheid. Een koninklijk besluit zou de nadere regels betreffende het gebruik van de gegevens van de Kruispuntbank moeten bepalen, in samenwerking met de Privacycommissie, die op 31 maart 2010 al adviseerde over het voorontwerp van deze wet (advies 14/2010).

Intussen werkt de wetgever aan het koninklijk besluit ter uitvoering van de Wet oprichting kruispuntbank van rijbewijzen. De Privacycommissie sprak zich op 6 juli 2011 uit over het ontwerp van dit koninklijk besluit. In haar advies merkt de Privacycommissie allereerst op dat er een onderscheid gemaakt moet worden tussen gegevensintegratie en dienstenintegratie. Het samenbrengen van alle gegevens met betrekking tot het rijbewijs is een vorm van gegevensintegratie, terwijl de klassieke Kruispuntbank – zoals vooral bekend in de vorm van de Kruispuntbank van de Sociale Zekerheid en het eHealth-platform – voornamelijk bedoeld was als dienstenintegrator met verwijzingsrepertoria. Indien beide functies geïntegreerd zouden worden in een enkele instantie – wat bij de Kruispuntbank van de rijbewijzen het geval lijkt te zijn, net als bij de Kruispuntbank van Ondernemingen – moeten deze rollen duidelijk afgebakend worden. Hoewel de Privacycommissie hieromtrent al een opmerking maakte bij het beoordelen van het ontwerp van de Wet tot oprichting van de kruispuntbank van de rijbewijzen, blijkt hier in de uiteindelijke wettekst onvoldoende rekening mee gehouden te zijn. Er wordt daarom allereerst geadviseerd om duidelijk te maken welke entiteit de authentieke bron is voor de gegevens die door andere instanties ter beschikking gesteld worden aan de Kruispuntbank van de rijbewijzen. Het ontwerp van het koninklijk besluit blijkt echter ook op verschillende vlakken onvoldoende rekening te houden met het onderscheid tussen gegevensintegratie en dienstenintegratie. Zo blijkt het ontwerp bij het bepalen van de bewaartermijnen van de gegevens dit onderscheid niet voldoende te vatten. Met betrekking tot de opname van medische gegevens in de Kruispuntbank van de rijbewijzen, een bijzondere categorie van persoonsgegevens, wordt opgemerkt dat één van de bijzondere uitzonderingsgronden voor de verwerking van dergelijke gegevens zal moeten worden toegepast, alsook dat er rekening gehouden moet worden met de specifieke voorwaarden tot dergelijke verwerking. Een meer fundamentele opmerking van